احراز هویت مرکزی
تجهیزات زیرساخت شبکه

تابستان ۱۳۹۲

رضا حجی زاده

hajjizadeh@gmail.com

طرح مسئله

با توجه به گستردگی شبکه های امروزی استفاده از ابزار ارتباط راه دور جهت مدیریت، پیکربندی و کنترل تجهیزات شبکه امری اجتناب ناپذیر است، البته این نوع ارتباط علاوه بر تسهیل و تسریع امور، امری چالش برانگیز است که ذهن هر مدیر شبکه ای را به خود مشغول کرده است. چه کسی حق دسترسی داشته باشد؟ هر کاربر[1] مجاز به انجام چه کارهایی است؟ هر کاربر در زمان ارتباط چه دستوراتی را اجرا کرده است؟ اینها مهمترین سئوالاتی است که مدیر امنیت شبکه باید به آنها پاسخ داده و روشی برای پیاده سازی آنها اتخاذ کند.

از مهمترین مسائل مورد توجه نحوه احراز هویت و میزان دسترسی افراد مجاز می باشد. جهت اتصال راه دور به تجهیزات سیسکو حداقل یک نام کاربری و کلمه عبور باید تعریف شود. برای نگهداری نام کاربری/کلمه عبور دو راه حل وجود دارد:

۱- دیتابیس محلی هر دستگاه
۲- یک سرویس دهنده مرکزی

استفاده از روش اول برای شبکه هایی با تعداد تجهیزات محدود قابل توجیه است، ولی زمانی را فرض کنید که لازم است یک نام کاربری اضافه یا یک کلمه عبور را برای تعداد زیادی سوئیچ و روتر تغییر دهید، در این صورت استفاده از روش دوم مقرون به صرفه و مطمئن تر[2] است.

[1] - وقتی در سطح مدیریت شبکه صحبت می شود منظور از کاربر همان مدیر شبکه است.
[2] - چون تنظیمات به ازاء هر دستگاه یک بار تکرار نمی شود، احتمال بروز خطای انسانی حین تایپ کردن نام کاربری/کلمه عبور وجود ندارد.

شرح وضعیت فعلی

در حال حاضر برای اتصال راه دور به سوئیچ ها و روترها از دیتابیس محلی هر دستگاه بصورت کاملا مستقل استفاده می‌شود.

برای استفاده از دیتابیس محلی چند راه حل وجود دارد:

۱- استفاده از کلمه عبور منحصر به فرد برای هر دستگاه
مزیت این روش حفظ محرمانگی و امنیت بیشتر برای دستگاه ها می باشد. در صورت افشای کلمه عبور یکی از دستگاه ها امکان اتصال به سایر تجهیزات برای فرد مهاجم امکان پذیر نیست.
عیب این روش زمانی است که تعداد تجهیزات زیاد باشد. در این حالت چون به خاطر سپردن این تعداد کلمه عبور مشکل است به ناچار باید آنها را در دفترچه یادداشت نوشت که آنهم مخاطرات خاص خود را دارد.

۲- استفاده از کلمه عبور واحد برای تمام دستگاه ها
این روش عیب حالت قبلی را ندارد ولی در عوض عیب بزرگتر آن است که در صورت دسترسی مهاجم به کلمه عبور امکان اتصال به تمام تجهیزات نیز برایش فراهم می باشد.

در شبکه فعلی از ترکیب دو حالت فوق استفاده می شود به این صورت که تجهیزات زیرساخت را به چند گروه (تجهیزات هسته مرکزی، سوئیچ های دفتر مرکزی، سوئیچ های شعب شهرستان، روترهای خارج کشور) تقسیم شده و برای هر گروه نام کاربری-کلمه عبور منحصر به فرد اختصاص داده شده است.

راه حل های موجود

تنها راه حل معقول و منطقی که هیچکدام از معایب روش فعلی مورد استفاده را ندارد، استفاده از یک سـرویس دهنـده متمرکز جهت احراز هویت می باشد.

برای پیاده سازی این روش دو پروتکل وجود دارد:

1- RADIUS
2- TACACS

در زمان احراز هویت مکانیزم عمل هر دو پروتکل یکسان است:

۱- کاربر درخواست برقراری ارتباط راه دور را برای سوئیچ/روتر ارسال می کند.
۲- خط فرمان نام کاربری-کلمه عبور ظاهر می شود.
۳- نام کاربری و کلمه عبوری که کاربر وارد کرده است برای سرور ارسال می شود.
۴- نتیجه (پذیرش/ رد ارتباط) صادر و برای سوئیچ/روتر ارسال می شود.

لازم به توضیح است هر یک از این پروتکلها علاوه بر احراز هـویت قابلیتهـای دیگـری نـیز در اختیـار مـدیر شـبکه قـرار می‌دهد:

۱- اعطای حق دسترسی متفاوت برای کاربران متفاوت
می توان برای مدیران شبکه که در واحدهای سازمانی[3] مختلف فعالیت می کننـد بنـا بـه نیـاز کـاری آن واحـد دسترسی منحصر به فردی ایجاد کرد.
۲- گزارش گیری از دستوراتی که کاربر در CLI[4] تایپ و اعمال می کند

[3] - **O**rganization **U**nit
[4] - **C**ommand **L**ine **I**nterface

مزایا/معایب روشهای پیشنهادی

جدول شماره ۱ مقایسه این دو سرویس دهنده می باشد:

Feature	RADIUS	TACACS
Layer 4 protocol	UDP	TCP
Encrypt transmission	Only Password	Entire session
Privilege modes support	Limited	15
Standard	Open Standard	Cisco Proprietary
Switch Memory Usage	Less	More than RADIUS
Architecture	Combine Authentication and Authorization	Separate AAA[5]
Authentication Method	Local, LDAP Server	Local, LDAP Server, Active Directory

جدول شماره ۱ – مقایسه RADIUS and TACACS

نتیجه گیری

همانطور که از جدول شماره ۱ استنباط می شود پروتکل TACACS نسبت به رقیب خود برتر است.

در خصوص گزارش گیری از دستورات ذکر این نکته ضروری است:

حالتی را در نظر بگیرید که دو کاربر همزمان در حال انجام تنظیمات روی یک دستگاه هستند. اگر گزارش‌گیری را با پروتکل RADIUS انجام دهید امکان تفکیک دستورات بر اساس نام کاربری وجود ندارد، حال آنکه این تفکیک با استفاده از پروتکل TACACS امکان پذیر است.

پیشنهاد می شود برای استفاده از قابلیت AAA تجهیزات سیسکو یک سرور TACACS+ نصب و برای احراز هویت از LDAP Server موجود استفاده شود.

با توجه به شرایط فعلی شرکت و سیاست نامه حق دسترسی می توان ترتیبی اتخاذ کرد که کارشناسان شعب نیز به تعداد محدودی دستور خط فرمان سوئیچ ها مانند show, debug دسترسی داشته باشند و بتوانند گزارشات را جهت رفع خطا مشاهده کنند.

با توجه به اینکه گزارشات سوئیچ به سرور Syslog ارسال می شود، گزارش دستورات اعمال شده روی سوئیچ به همان سرور TACACS+ منتقل شود.

[5] - **A**uthentication **A**uthorization **A**ccounting

جزئیات پیاده‌سازی پیشنهادی

سخت افزار مورد نیاز: یک سرور فیزیکی/مجازی با حداقل مشخصات زیر:

- CPU: 3 GHz
- RAM: 2GB
- H.D.D: 30 GB

نوع پروتکل: tacacs

سرویس دهنده: یکی از سرویس دهنده های نرم افزاری متن باز[۶]

مکانیزم حراز هویت: استفاده از سرویس دهنده LDAP موجود

محدوده تحت پوشش: تمامی تجهیزات زیرساخت شبکه اعم از سوئیچ ها و روتر هایی که در سطح شرکت یا از طریق پروتکل های تونل لایه ۲ به شبکه مرکزی متصل شده اند.

مکانیزم برقراری امنیت: تامین امنیت سیستم عامل مانند نصب آخرین بروزرسانی ها، حذف سرویس های غیرضروری و همچنین استفاده از لیست کنترل دسترسی[۷] که فقط به VLAN مدیریت سوئیچ ها اجازه دسترسی به سرور را می دهد و از طریق سوئیچ لایه توزیع[۸] مرکزی بر روی ترافیک شبکه اعمال می شود.

---

[6] - Open Source
[7] - Access Control List(ACL)
[8] -Distribution Layer